UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA **Plaintiff** **v.** **PHILIP M. POPA, JR.,** **Defendant**	**CASE NOS.: 5:18-CR-448** **JUDGE BENITA Y. PEARSON** **MOTION TO SUPPRESS AND MOTION TO SUPPLEMENT** ***Hearing requested***

Now comes the Defendant Philip M. Popa, Jr., by and through the undersigned counsel, and hereby moves this Court to suppress the search conducted on July 18, 2018 and all the evidence gained therefrom, including but not limited to computers and statements by the Defendant Philip Popa. The warrant was not supported by probable cause, information contained in the Affidavit was obtained in violation of Mr. Popa's Fourth Amendment right, and the Affidavit contained false and/or misleading statements. This Motion is supported by the Memorandum in Support, which is attached hereto and incorporated herein by express reference. Additionally, Mr. Popa requests leave to supplement this Motion upon receipt of an expert report from Tami Loehrs of Loehrs & Associates, L.L.C. Simultaneous with the filing of this Motion, Mr. Popa is filing a motion to have Ms. Loehrs appointed as an expert in this matter and to compel software necessary for her to perform an independent forensic analysis.

Respectfully submitted,
WILLIAM T. WHITAKER CO. LPA
/s/Andrea Whitaker
ANDREA WHITAKER #0074461
54 E. Mill Street Suite 301
Akron, Ohio 44308
T: 330-762-0287 F: 330-762-2669
whitaker@whitakerlawlpa.com
Attorney for Defendant

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was electronically filed this 11th day of February, 2019. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system.

/s/ Andrea Whitaker
Andrea Whitaker

MEMORANDUM IN SUPPORT

I. FACTS

Defendant John Popa is charged with one count receipt of visual depictions of real minors engaged in sexually explicit conduct in violation of 18 U.S.C. § 2252(a)(2) and one count of possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). The Government's discovery response and Affidavit in Support of the Search Warrant refer to Freenet as the computer software program used by law enforcement and an Administrative subpoena used to obtain the physical location of an IP address.

On July 17, 2018, Ryan D. Anschutz, a Task Force Officer in the Federal Bureau of Investigation applied for a search warrant to search and seize evidence at 533 Redwood St SW, Beach City, Ohio 44608. See Search Warrant and Affidavit attached hereto as Exhibit A. The request for a warrant was supported by an affidavit signed by Agent Anschutz. In the affidavit, the Affiant (Agent Anschutz) avers that there is probable cause to believe that a user of an IP address at this address has received, possessed, and/or distributed child pornography. Ex., A, Affidavit in Support of Search Warrant ("Affidavit"), ¶ 3. The Affidavit contains the Affiant's experience, a description of the place to be searched and the items to be seized, and definitions of terms contained there.

The Affidavit also contains an explanation of "Freenet." According to the Affiant, it is "an Internet-based, peer-to-peer (P2P) network that allows users to anonymously share files, chat on message boards, and access websites within the network." Affidavit, ¶7. The Affiant further explains that in "order to access Freenet, a user must first download the Freenet software, which is free and publicly available. The Freenet 'source code" - i.e., the computer programming code that facilitates Freenel's operation - is also publicly available. In other words, Freenet is 'open

source" software that may be examined and analyzed by anyone with the pertinent expertise or knowledge." Id. at ¶ 8. The Affidavit then goes on to explain a Freenet user may be an "original requestor" of a file or one that "is merely forwarding the request of another user." Id. at ¶ 12.

This fact, and the Affiant's knowledge of it, is of the upmost importance because it indicates that some "requests" for files, including child pornography, happen without the users' knowledge or consent. The Affiant recognizes that law enforcement must be able to distinguish between the two types of requests in order to identify where there is probable cause that a user is requesting illegal material. Id. The Affiant identifies a "peer-reviewed, publicly-available academic paper describing the methodology of" a mathematical formula upon which he claims to rely to make this important determination. Affidavit, ¶ 24. While the Government has provided the paper to the undersigned, there has been no response to the request for evidence that the paper was, in fact, peer-reviewed or found to be reliable in any way. The undersigned has been unable to locate any such information in her own research.

This is important because the Affiant recognizes that "Freenet attempts to hide which computer uploaded a file into or downloaded a file from the network by making it difficult to differentiate whether a request for a piece that comes in from a peer originated with that peer (Le., the peer was the "original requestor" of the file), or whether that peer was simply forwarding a different peer's request." Id. at ¶ 14. "Freenet attempts to hide the identity of the original requestor by randomizing the initial number of times a request can be forwarded from one peer to another to be either 17 or 18. Without this randomization, any time a user received a request for a piece of a file that could be forwarded 18 times, the user would know that its peer was the original requestor of the file." Id.

According to the Affidavit, a "modified version of the Freenet software is available to sworn law enforcement officers to assist in conducting Freenet investigations." Id. at ¶ 20. Using that modified version of Freenet, in April, 2018, Agent Anschutz identified "a computer running Freenet software, with an IP address of 173.90.126.69, with 13.1 peers, requested from a law enforcement computer 136 out of 1786 total pieces needed to assemble a file with a SHA1 digital hash value of ATLOOVASIDQV6JPNOK4Z3MTKWGYFYS6W." Affidavit, ¶ 27. In other words, the computer at the suspect IP address reportedly requested less than .075% of a file. Officer Anschutz then downloaded the completed file from another source and described the completed file in the Affidavit. Id. This activity occurred for several additional files. Id. at ¶¶ 28-29.

The Affidavit then indicates that "[u]sing publicly available search tools, law enforcement determined that IP address 173.90.126.69 was controlled by Internet Service Provider ("ISP') Time Warner Cable." Id. at 32. The Affiant then issued an administrative subpoena sent "Time Warner Cable for the date and times that the above-described files were downloaded" and found that the "IP address was assigned to the account registered to 'James Skelly,' at the PREMISES, email addresswowsaddie@twc.com. Telephone number 330-324-4421, account number 206389203 and the active IP address date of 12119/2017." Id. at 33

Thereafter, Agent Anschutz prepared the Affidavit in support of his request for a search warrant on July 17, 2018. The Affidavit was submitted to and approved by a Magistrate Judge of the United States District Court for the Northern District of Ohio that same day. On July 17, 2018, law enforcement officers executed the search warrant at Mr. Popa's residence and seized several items, which were subsequently forensically analyzed by law enforcement agents. Law enforcement officers also arrested and obtained a statement from Mr. Popa.

As a result of the Government's investigation in this case, Mr. Popa was indicted on August 14, 2018 with the foregoing offenses. After receiving the Government's initial discovery response, defense counsel retained the services of a local expert at defense counsel's expense. Consultation with the expert and a review of the discovery identified several issues for pretrial motions. However, the expert had little experience with Freenet. Mr. Popa's counsel requested a copy of the law enforcement modified version of Freenet. The Government indicated that the law enforcement software was not discoverable.

As the undersigned was preparing the pretrial motions, she was referred to Tami Loehrs of Loehrs & Associates, L.L.C. as someone with potentially more experience with Freenet. The undersigned immediately contacted Ms. Loehrs and provided her with a copy of the discovery to determine if additional issues were significant to Mr. Popa's defense. Ms. Loehrs reviewed the discovery and provided an Affidavit of her initial findings. See Affidavit of Tami Loehrs (TL Affidavit") attached hereto as Exhibit B. Ms. Loehrs identified several issues heretofore unknown to the undersigned and indicated that it would be necessary to conduct an independent forensic examination of the electronic evidence that was seized in connection with the search warrants. Ms. Loehrs has extensive experience conducting forensic examinations in child pornography cases and is acutely familiar with the investigative aspects of such cases, including the Government's use of specialized forensic software. Simultaneously with the filing of this Motion, Mr. Popa is filing a Motion to Suppress, with leave to supplement, and a Motion to Appoint Ms. Loehrs as an expert for Mr. Popa.

Based upon her review of the evidence as well as her prior experience with law enforcement's use of modified software programs, Ms. Loehrs opines that an independent forensic examination of the law enforcement version of the Freenet Software is necessary in order to

determine the validity and/or reliability of the Government's forensic evidence and to assess the information provided in the Affidavit in support of the search warrant. As she notes, in her "forensic training, some of which has come directly from law enforcement, [she has] been taught that [she] cannot rely on a tool (software) that has not been properly tested and validated by [her] and is not available for testing and validation by [her] industry peers." TL Aff., ¶ 21. Ms. Loerhs, however, goes farther than to just note that it is best practice, as noted herein, she identifies specific concerns regarding the law enforcement Freenet that require an independent analysis.

Specifically, Ms. Loehrs notes that she has "worked on hundreds of cases throughout the country involving law enforcement's investigations of P2P and BitTorrent file sharing networks, including the use of Freenet, which has brought to light serious issues with regard to the accuracy and reliability of the proprietary software used by law enforcement to conduct these investigations and whether that software is going beyond information that is publicly available as well as reporting false information regarding files that do not exist on a suspect computer and/or do not contain child pornography." TL Aff, ¶ 7. She is concerned that, in "spite of this, Officer Anschutz avers in his Affidavit that the IP address associated with Mr. Popa contains child pornography based on incomplete files reported by his law enforcement tool and then describes completed files that he downloaded from other sources." Id. at 15.

Agent Anschutz refers to the "law enforcement's tool" used to analyze the network and an allegedly peer reviewed article that allow him to come to the conclusion that is significantly more probable than not that the suspect IP address was the original requestor of the child pornography files. As noted above, this is crucial to a finding of probable cause because the Agent notes that without such a tool, there is no way to know if a Freenet user is actually requesting anything illegal. "Officer Anschutz provides no information regarding 'law enforcements tool', including whether

that tool has been tested and validated, nor does he provide any log files created by the law enforcement tool as foundation for his opinions." T.L. Aff, ¶ 16.

II. LAW AND ARGUMENT

The Fourth Amendment to the U.S. Constitution grants Defendants the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." This right has been incorporated against the states through the Fourteenth Amendment and is reiterated by Article 1, Section 10 of the Ohio Constitution. It is well-established that "all evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in state court." *Mapp v. Ohio*, 367 U.S. 643, 655 (1961). Put differently, any evidence seized pursuant to an invalid search warrant must be excluded at trial. *Franks v. Delaware*, 438 U.S. 154, 155 (1978).

A. THE WARRANT WAS SUPPORTED BY INFORMATION OBTAINED IN VIOLATION OF MR. POPA'S FOURTH AMENDMENT RIGHT TO BE FREE FROM UNREASONABLE SEARCH AND SEIZURE

The warrant to search the house and seize Mr. Popa's computer was supported by information obtained in violation of Mr. Popa's Fourth Amendment right. In the Affidavit, the Affiant indicates that he is requesting to search the particular address because an administrative subpoena indicated that the address was the location of the IP address the Affiant was investigating. He stated that "[u]sing publicly available search tools, law enforcement determined that IP address 173.90.126.69 was controlled by Internet Service Provider ("ISP') Time Warner Cable." Id. at 32. The Affiant then sent an administrative subpoena to "Time Warner Cable for the date and times that the above-described files were downloaded" and found that the "IP address was assigned to the account registered to 'James Skelly,' at the PREMISES, email addresswowsaddie@twc.com.

Telephone number 330-324-4421, account number 206389203 and the active IP address date of 12119/2017." Id. at 33.

Before the execution of the search warrant at issue in this case, the United States Supreme Court issued its Decision in *Carpenter v. United States* (2018), 585 U.S. ____. *Carpenter* reconsidered the third-party doctrine developed in *Smith v. Maryland*, 442 U.S. 735 (1979) in the digital age. In *Smith*, the Supreme Court found that an individual did not have a reasonable expectation of privacy in the numbers recorded by a pen registry. This decision established the third-party doctrine: if information is freely given to a third party, the police are not required to obtain a warrant. In *Carpenter*, the Court reversed the Sixth Circuit Court of Appeals and held that a warrant was required for police to access cell site location information from a cell phone company (the detailed geolocation information generated by a cellphone's communication with cell towers.) The Court recognized that there are circumstances when people have a valid expectation of privacy in information that is stored with a third party.

"[B]oth empirical research and public opinion polls suggest that the public has higher expectations of privacy than those recognized by the courts in most Fourth Amendment jurisprudence." Christine Scott-Hayward et al., Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age, 43 Am. J. Crim. L. 19, 49 (2015). *Carpenter* was a continued extension of the Court's recognizing this changing landscape. See, e.g., *Riley v. California*, 134 S. Ct. 2473 (2014) (warrantless search incident to arrest may not include search of digital information on the arrested person's cell phone.) In fact, the Supreme Court in *Riley* specified that one reason a warrant was required for searches of mobile telephones, even in a search incident to arrest, was because "[a]n Internet search and browsing history, for example, can be

found on an Internet-enabled phone and could reveal an individual's private interests or concerns." *Riley*, 134 S. Ct. at 2490.

In *United States v. Jones*, 565 U.S. 400, 417-18 (2012), Justice Sotomayor discussed the third-party doctrine in these changing times. She found that the doctrine "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties" such as "the URLs that they visit" and observed that "I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year."

Justice Gorsuch's dissent in *Carpenter* would appear to make this abandonment of the third-party doctrine even clearer. He expressed disappointment that the third-party doctrine was not more broadly revisited. Although a dissent on procedural grounds, the opinion goes even farther in distancing the Court from the third-party doctrine. It unambiguously agrees with the majority that "the rationale of Smith and Miller is wrong" and recognized a property right interest in information stored with third-parties.

> [T]he fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them. Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a bailment. A bailment is the "delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose." Black's Law Dictionary 169 (10th ed. 2014); J. Story, Commentaries on the Law of Bailments §2, p. 2 (1832) ("a bailment is a delivery of a thing in trust for some special object or purpose, and upon a contract, expressed or implied, to conform to the object or purpose of the trust"). A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the "implication[s] from their conduct" if they don't…A bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable for conversion…
>
> These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a

> third party may not mean you lose any Fourth Amendment interest in its contents. Whatever may be left of *Smith* and *Miller*, few doubt that e-mail should be treated much like the traditional mail it has largely supplanted— as a bailment in which the owner retains a vital and protected legal interest…
> Id. at 14 (Gorsuch dissenting).

Justice Gorsuch says, explicitly, that it is "entirely possible a person's cell-site data could qualify as his papers or effects under existing law." Id. at 20 (Gorsuch dissenting).

The administrative subpoena issued in the instant case for the information stored at Time Warner is akin to the information at issue in *Carpenter* and, therefore, the Government obtained it in violation of Mr. Popa's Fourth Amendment right. Using a subpoena to acquire records related to the IP address from a third party, Time Warner, constituted a Fourth Amendment search.

B. THE AFFIDAVIT DOES NOT CONTAIN FACTS SUFFICIENT FOR PROBABLE CAUSE AND CONTAINS MATERIAL MISREPRESENTATIONS

The Affidavit only indicates that a fraction of a file was downloaded by the IP address it was investigating. This is not enough for an issuing Magistrate to find probable cause that a user of that IP address was in possession of illegal material. The Affidavit indicates that the "suspect IP address reportedly requested less than .075% of a file which would likely render that file non-viewable and would not, in that incomplete state, contain child pornography." TL Affidavit, ¶ 6. The Affiant then indicates that he "downloaded the completed file from someone other than the suspect and describes the content of the completed file in his Affidavit. This activity occurred for several additional files, none of which the suspect reported having 100% of the content." Id. The Affidavit, however, does not provide any basis to believe that the entire file would be located on the suspect computer except for the workings of a mathematical formula on which the Affiant claims to have relied.

The Affiant plainly states that there would be no basis to know or even assume that the IP address he was investigating was the original requestor of illegal material without the mathematical

formula he obtained from the "peer-reviewed" article. Affidavit, ¶ 24. He basis for relying on this formula is the claim that the article is peer-reviewed. However, the article does not appear in any journal the undersigned can locate nor does any research in to the article indicate that it was peer-reviewed. This may be because the formula the article claims as sound is not. See Exhibit C. While the attached article is published by Freenet, Mr. Popa will present additional evidence, including the testimony of Ms. Loehrs, to support this position. Mr. Popa also seeks leave to supplement this portion of the Motion to Suppress until after Ms. Loehrs has completed her review and provided her report.

In *Franks v. Delaware* (1978), 438 U.S. 154, the United States Supreme Court held that probable cause cannot rely upon statements in an affidavit that are knowingly false or exhibit a reckless disregard for truth. In *Franks*, the Supreme Court held that, if the removal of the false statement or statements made in reckless disregard for the truth results in insufficient facts to establish probable cause, the evidence seized under the warrant is subject to exclusion. Id. Omissions count as a false statement if they are designed to mislead, or are made in reckless disregard of whether they would mislead. Further, "the validity of the warrant must be assessed on the basis of the information that the officers disclosed, or had a duty to discover and disclose." *Marilyn v. Garrison* (1987), 480 U.S. 79, 85. If there is a "substantial preliminary showing" that a false statement was included in the affidavit, a Court must give a defendant an opportunity to cross examine the Affiant and the defendant then must demonstrate by a preponderance of the evidence that the misstatements were made knowingly, or with a reckless disregard for the truth. Id.

In the Affidavit in support of the search warrant, the Affiant claims that the formula that allows him to point the address of Mr. Popa as the source of the request for illegal material is

reliable because it is has been vetted by a peer-review process. This does not appear to be true. Mr. Popa respectfully requests a hearing on this matter.

III. CONCLUSION

Finally, as noted above, simultaneous with the filing of this Motion, Mr. Popa is requesting that the Court appoint Tami Loehrs as an expert in this matter. Mr. Popa hereby requests leave to supplement the Motion to Suppress until such time as Ms. Loehrs has completed her review of the discovery and conducted an independent forensic analysis of the evidence seized by the Government. While Mr. Popa understands that this matter has been pending, he seeks additional time to allow the undersigned to provide effective assistance of counsel. He has previously waived his right to a speedy trial and he is being held without bond so there are no concerns about his attendance at hearings if there is a further delay. Mr. Popa requests a hearing on this Motion as well.

Respectfully submitted,
WILLIAM T. WHITAKER CO. LPA

/s/Andrea Whitaker
ANDREA WHITAKER #0074461
54 E. Mill Street Suite 301
Akron, Ohio 44308
T: 330-762-0287 F: 330-762-2669
whitaker@whitakerlawlpa.com
Attorney for Defendant